Zentrale Serverüberwachung im Windows-Netzwerk

Manuel Selling | manuel.selling@cms.hu-berlin.de

In einem großen Netz, wie dem der Humboldt-Universität, ist es nicht leicht für die Administratoren, den Überblick zu behalten. Eine Vielzahl von verschiedenen Servern ist bereitzustellen und deren Funktionen sind zuverlässig anzubieten. Doch wie soll das sicher und effizient bewerkstelligt werden? In solchen Fällen bietet es sich an, zu Tools zu greifen, die dem Administrator die Arbeit erleichtern. Eines dieser eingesetzten Tools ist das System- und Netzwerk-Monitoring-Tool Nagios, dessen Einsatzmöglichkeiten am Beispiel des zentralen Windows-Netzwerkes der HU vorgestellt werden sollen.

Das universitätsweite Windows-Netz besteht aus 40 produktiven Domänen-Controllern (DC) und 24 Fileservern zur Versorgung von 17 Domänen. Dazu gehören noch 17 Domänen-Controller und 3 Fileserver im Testnetz. Da ein Großteil der Domänencontroller des Windows-Netzwerkes virtualisiert wurde, gehören die entsprechenden Virtualisierungshosts auch zu den zentralen Komponenten des Windows-Netzes, die zu überwachen sind. Dazu kommen noch einige Hilfssysteme und Dienste. Die meisten dieser Server bieten nicht nur einen Service an, sondern eine Vielzahl von Diensten.

Um hier nicht den Überblick zu verlieren und eine schnelle und einfache Übersicht unserer Systeme und deren Gesundheitszustand zu erhalten, nutzen wir Nagios. Nagios ist eine Opensource-Software, welche ständig – durch die Community unterstützt – weiterentwickelt wird.

Warum Monitoring?

Hauptzweck der Überwachung unserer Systeme ist die zeitnahe Benachrichtigung bei Ausfällen, um schnellstmöglich reagieren zu können. Nur so lässt sich ein Betrieb mit möglichst geringen Ausfallzeiten gewährleisten. Das Monitoring mit Nagios ermöglicht uns auch das Erkennen von Problemen vor einer Havarie. Das hilft uns unter Umständen, einen völligen Ausfall zu vermeiden und die nötigen Entscheidungen zu treffen. Ein weiterer Bestandteil der Überwachung mit Nagios ist es, eine gesamte Sicht über das vorhandene Netzwerk zu gewinnen und dessen Vitalitätszustand zu visualisieren. Das vereinfacht bei einem Ausfall die Fehlersuche und Lokalisierung.

Eine Arbeitserleichterung im täglichen Betrieb verschaffen uns die Automatisierung von Routineaufgaben und die Erkennung von langfristigen Trends.[1] Zum Beispiel können wir so feststellen, inwieweit die Kapazität der von unseren Fileservern zur Verfügung gestellten Festplatten ausgeschöpft ist und wie der Trend der Zunahme der Daten auf diesen Platten ist. Stellen wir eine kontinuierliche Zunahme fest, können wir darauf entsprechend reagieren, die Administratoren der Einrichtungen bzw. Institute informieren und Maßnahmen treffen.

Aufbau und Konzept von Nagios

Im Grobkonzept ist Nagios ein Framework zur Verwaltung von Überprüfungen (Checks) und Benachrichtigungen (Notifications).[2] Über eine Plugin-Schnittstelle führt die Software Checks und Notifications aus. Die Ergebnisse der Checks werden aufbereitet in einem Web-Frontend zur Verfügung gestellt. Die Abbildung 1 stellt den vereinfachten Ablauf dar.

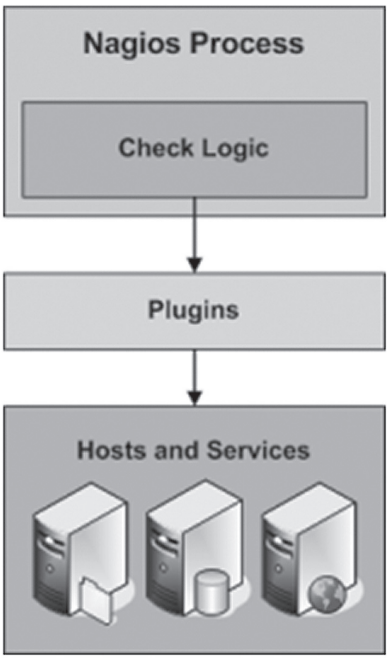

Abb. 1: Einfache schematische Darstellung von Nagios-Checks [3]

Etwas detaillierter wird der grundsätzliche Ablauf in der Abb. 2 dargestellt. Dort ist erkennbar, welche Zustandsmeldungen („ok“, „warning“, „critical“) vom Nagios-Plugin zurückgegeben werden und wie diese durch zusätzliche Informationen aufgewertet werden.

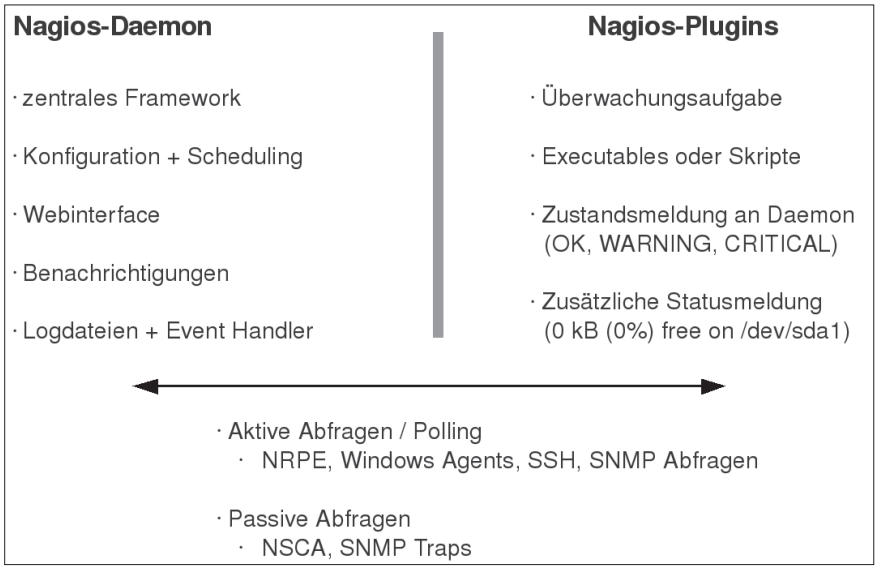

Abb. 2: Grundsätzlicher Aufbau von Nagios [1]

Viele Hersteller und freie Entwickler stellen Plugins bereit, die spezielle Hardware und Dienste prüfen. Die Ergebnisse werden dann „Nagios-konform“ ausgeliefert. Somit werden sehr viele Schnittstellen zu unterschiedlichen Systemen (z. B. Datenbanken, Applikationsservern, Sun-Server, Dell-Server usw.) geliefert. Man kann auch selber Plugins schreiben, um spezielle Anforderungen abzudecken.

Kernkomponenten des Windows-Netzwerkes der HU

Die zentralen Komponenten des Windows-Netzwerkes, die mit Nagios überwacht werden, sind Domänen-Controller und Fileserver.

Domänencontroller stellen den Active Directory-Dienst bereit. Das ist ein Verzeichnisdienst, der für die Verwaltung der Benutzeraccounts im Windows-Netz der HU verantwortlich ist. Vereinfacht gesagt: Nutzer einer Domäne melden sich an den Domänencontrollern an und erhalten nach erfolgreicher Authentifizierung berechtigten Zugriff z. B. auf ihre Homeverzeichnisse oder Projektlaufwerke. Die Domänencontroller stehen redundant zur Verfügung, um eine optimale Ausfallsicherheit zu gewährleisten. Trotzdem müssen wir bei Ausfall eines Domänencontrollers unverzüglich informiert werden, da ansonsten bei Problemen mit dem zweiten Domänen-Controller die gesamte Domäne gefährdet wäre.

Auf den Fileservern werden die aus dem SAN gelieferten Festplattenkapazitäten verwaltet und dem Nutzer zur Verfügung gestellt. Die physischen Fileserver (Nodes) einer Domäne sind zu einem Cluster verbunden. Mit Hilfe der Cluster-Software ist es möglich, die SAN-Platten, Shares und Skripte an jedem physischen Mitglieds-Node des Clusters bereitzustellen. Die Cluster-Ressourcen werden immer über die virtuellen Cluster-Adressen angesprochen. Um zu überprüfen, ob diese für die Nutzer erreichbar sind, werden sie auch mittels Nagios überwacht.

Durch die umgesetzte Strategie der Virtualisierung im Bereich der Domänencontroller müssen auch die dazugehörigen VM-Hosts, also jene Server, die die Domänencontroller als virtuelle Maschinen (Gäste) beherbergen, überwacht werden.

Um die Gesamtheit des Windows-Netzes zu erfassen und dessen Abhängigkeiten zu bestimmen, werden auch noch die Infrastruktur-Komponenten des Netzwerkes (z. B. Switche, Router) in die Nagios-Überwachung einbezogen.

Überprüfung der Kernkomponenten durch Nagios

Netzwerk

Wenn ein Host/Server/Dienst nicht erreichbar ist, muss es nicht immer am Server selbst liegen. Es kommt häufig vor, dass Infrastruktur-Komponenten, die vor dem eigentlichen Server liegen, Probleme haben (nicht erreichbar sind) und somit der Server nicht erreichbar ist. Die Logik von Nagios berücksichtigt das, indem bei jedem zu überprüfenden Host der jeweilige Vorgänger oder Parent angegeben wird. Bei einem negativen Check des Hosts (nicht erreichbar) wird zu allererst geprüft, ob der eingetragene Parent erreichbar ist. Ist dieser auch nicht erreichbar, prüft Nagios nicht mehr die einzelnen Services des eigentlichen Hosts, sondern markiert ihn als „critical“ und verschickt in bestimmten konfigurierten Intervallen Benachrichtigungen (Mail, SMS) an die jeweiligen Administratoren.[4] Somit können Abhängigkeiten und Eskalationsverhalten definiert und angewendet werden. Die häufigsten Parents sind in unserer Konfiguration Router und Switche bzw. im zunehmenden Maße die VM-Hosts.

Für unsere Zwecke reicht es aus, die Verfügbarkeit der verwendeten Netzwerkkomponenten zu prüfen. Dafür können wir den in Nagios integrierten Host-Check (*check-host-alive*) nutzen, der wiederum das Plugin *check_ping* benutzt (s. Abb. 3).

Host	Service	Status	Last Check	Duration	Attempt	Status Information
gateway-ahof	PING	OK	29-03-2010 15:00:28	16d 21h 55m 23s	1/3	PING OK - Packet loss = 0%, RTA = 0.62 ms

Abb. 3: Ergebnis des check_ping Plugins nach der Überprüfung eines Routers

VM-Host

Als Host für die meisten unserer Domänencontroller dienen Virtualisierungsserver auf VMware-Basis. Ein Skript auf dem jeweiligen VM-Host ermittelt die von uns benötigten Daten über die notwendigen Dienste und Eigenschaften. Momentan werden die Zustände folgender Services und Eigenschaften durch Nagios geprüft:

- Plattenplatzbelegung (Mountpoints)
- HTTPS
- CPU Load (wie sind die CPUs ausgelastet)
- verschiedene Services/Daemons (z. B. sshd, ntpd, dsmcd)
- SSH
- RAM-Ausnutzung

Domänencontroller

Für die allgemeine Überprüfung der Domänencontroller verwenden wir das Plugin *check-nt*. Es nutzt den Windows internen Performance Counter und überprüft in unserem Falle folgende Parameter des Hosts und liefert deren Status zurück:

- Plattenplatzbelegung der lokalen Platten
- CPU Load
- RAM-Ausnutzung
- definierte Services, die gestartet sein sollten
- Active Directory

Für die Übermittlung der Ergebnisse verwenden wir den NSClient++, er kann auch über das Plugin *check_nrpe* angesprochen werden, um zusätzlich eigene Skripte ausführen und auswerten zu lassen.[2] Ein solches Skript ist *check_ad*. Es führt auf dem Domänencontroller ein Diagnose-Tool aus (dcdiag.exe) und bereitet die Ergebnisse für Nagios auf (Abb. 4).

Der NSClient++ ist somit die Übermittlungsschnittstelle der ausgeführten Plugins und Checks zum Nagios-Server.

Fileserver und Cluster-Nodes

Der Check für die Fileserver soll uns einen allgemeinen Überblick über den Gesundheitszustand der physischen Cluster-Nodes geben. Es werden nur folgende lokale Parameter geprüft:

- Plattenplatzbelegung der lokalen Platten
- CPU Load
- RAM-Ausnutzung
- definierte Services, die gestartet sein sollten

Mit der Überprüfung der virtuellen Cluster-Nodes, das sind die Cluster-Nodes, die die Cluster-Ressourcen für Nutzer bereitstellen, erhalten wir detaillierte Informationen über den Zustand bzw. die Auslastung des angebotenen File-Service. Es wird die Auslastung der zur Verfügung gestellten SAN-Platten überprüft (gesamter/benutzter/freier Platz). In den Konfigurationsdateien von Nagios werden die Schwellwerte definiert, so dass z. B. der Zustand von „ok“ zu „warning“ wechselt, wenn nur noch 20% der Platten frei sind. Der Administrator wird dann per Mail informiert und kann entsprechend reagieren. Des Weiteren werden noch weitere Cluster-Ressourcen geprüft, u. a. abhängige Dienste, die gestartet sein müssen (z. B. TSM-Dienst, Dienste zum automatischen Anlegen von Homeverzeichnissen).

Fazit

Es gibt eine Vielzahl von Plugins der Hersteller von Servern (z. B. Dell), mit deren Hilfe die meisten Sensor- und Hardwaredaten (z. B. Lüfter, Temperatur, RAID-Status) an Nagios gesendet und überwacht werden können. Die Abbildung 6 zeigt die Ergebnisse des *check_openmanage*-Plugins.

Es gibt nicht nur den RAID-Status des Servers zurück, sondern liefert auch noch Performancedaten von den Lüfter-, Strom- und Temperatursensoren. Mit Hilfe des PNP4Nagios-Addons lassen sich daraus komfortabel Trends, Statistiken und Analysen herleiten (siehe Abb. 7).[5]

Zum Abschluss ist zu sagen, dass man mit Nagios und den dazugehörigen Schnittstellen (Plugins, Skripte usw.) fast alles überwachen kann. Dazu gehört auch die Möglichkeit, eigene Skripte zu

Service	Status	Last Check	Duration	Attempt	Status Information
ACTIVE DIRECTORY	OK	31-03-2010 12:19:24	11d 12h 51m 51s	1/3	AD OK - Connectivity OK, Services OK, Replications OK, Advertising OK, Fsmo OK, Rid Manager OK, Machine account OK, FRS Sysvol OK, FRS Event OK, KCC Event OK

Abb. 4: Status der Rückgabe des check_ad Skripts

Service	Status	Last Check	Duration	Attempt	Status Information
DISK_USAGE_I	OK	31-03-2010 13:17:45	187d 2h 14m 42s	1/3	J:\ - total: 399.99 Gb - used: 303.05 Gb (76%) - free 96.94 Gb (24%)
DISK_USAGE_K	OK	31-03-2010 13:17:45	187d 1h 35m 7s	1/3	K:\ - total: 399.99 Gb - used: 286.58 Gb (72%) - free 113.41 Gb (28%)
DISK_USAGE_L	OK	31-03-2010 15:07:34	106d 13h 57m 28s	1/3	L:\ - total: 239.98 Gb - used: 177.97 Gb (74%) - free 62.01 Gb (26%)
DISK_USAGE_M	WARNING	31-03-2010 10:52:31	46d 18h 27m 11s	3/3	M:\ - total: 149.99 Gb - used: 121.44 Gb (81%) - free 28.55 Gb (19%)
DISK_USAGE_N	OK	31-03-2010 11:28:10	357d 6h 26m 6s	1/3	N:\ - total: 249.99 Gb - used: 78.15 Gb (31%) - free 171.84 Gb (69%)
SERVICESTATE	OK	31-03-2010 14:29:29	106d 13h 48m 37s	1/3	TSM-Scheduler Service Group 3: Started

Abb. 5: Critical-State der Plattenplatzbelegung bei einem virtuellen Cluster-Node

Service State Information	
Current Status:	OK (for 9d 1h 6m 48s)
Status Information:	OK - System: 'PowerEdge R610', SN: '[redacted]', hardware working fine, 1 logical drives, 2 physical drives
Performance Data:	'fan_0_system_board_fan_mod_1a_rpm'=4320RPM;0;0 'fan_10_system_board_fan_mod_5b_rpm'=3120RPM;0;0 'fan_11_system_board_fan_mod_6b_rpm'=3360RPM;0;0 'fan_1_system_board_fan_mod_2a_rpm'=4440RPM;0;0 'fan_2_system_board_fan_mod_3a_rpm'=4560RPM;0;0 'fan_3_system_board_fan_mod_4a_rpm'=4440RPM;0;0 'fan_4_system_board_fan_mod_5a_rpm'=4440RPM;0;0 'fan_5_system_board_fan_mod_6a_rpm'=4320RPM;0;0 'fan_6_system_board_fan_mod_1b_rpm'=3000RPM;0;0 'fan_7_system_board_fan_mod_2b_rpm'=3000RPM;0;0 'fan_8_system_board_fan_mod_3b_rpm'=3120RPM;0;0 'fan_9_system_board_fan_mod_4b_rpm'=3120RPM;0;0 'pwr_mon_0_ps_1_current_1'=0.2A;0;0 'pwr_mon_1_ps_2_current_2'=0.4A;0;0 'pwr_mon_2_system_board_system_level'=147W;917;966 'temp_0_system_board_ambient'=19C;42;47
Current Attempt:	1/4 (HARD state)

Abb. 6: Check-Ergebnisse des check_openmanage-Plugins

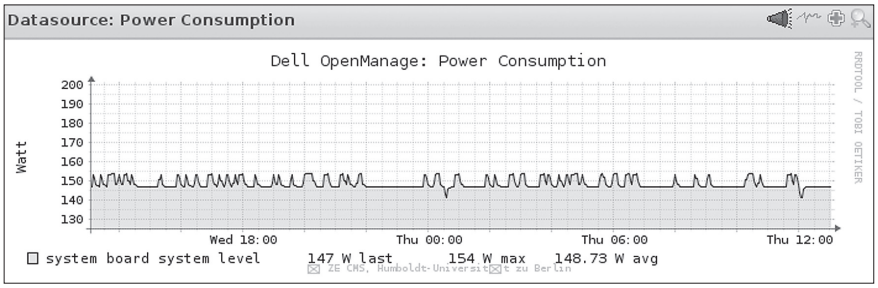

Abb. 7: Grafische Darstellung der Leistungsaufnahme mit Hilfe von pnp4nagios

entwickeln. Durch die vorgestellten und eingesetzten Funktionen von Nagios ist es uns möglich, einen Gesamtüberblick über den Gesundheitsstatus des Windows-Netzwerkes zu gewinnen (siehe Abb. 8).

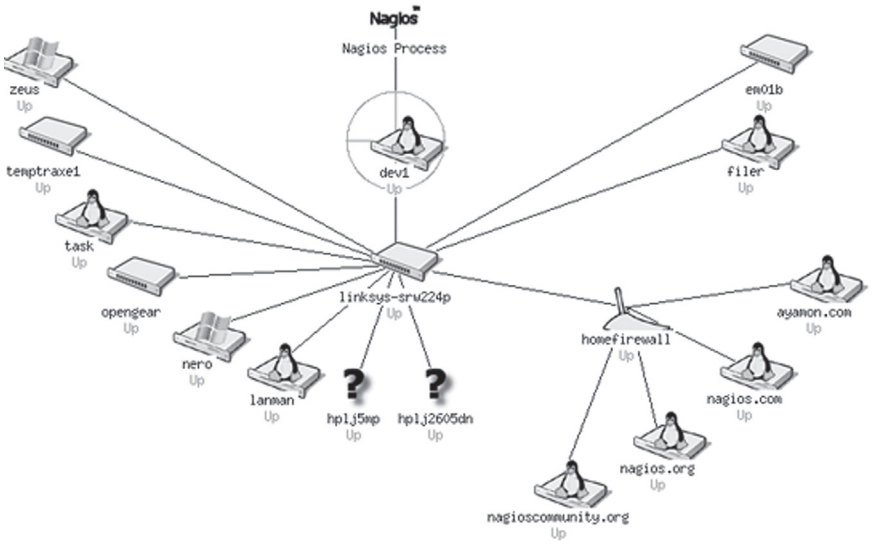

Abb. 8: Das Netzwerk auf einen Blick [3]

Literatur

[1] http://blog.netways.de/wp-content/uploads/2008/01/nagios-heise-osmb-2008-v11.pdf, 12.04.2010

[2] http://velt.de/system/files/Nagios-Vorstellung.pdf, 12.04.2010

[3] http://www.flickr.com, 12.04.2010

[4] http://www.nagios.org, 12.04.2020

[5] http://www.pnp4nagios.org, 12.04.2010